HP Sure Yönetici Kullanıcı Kılavuzu

ÖZET

HP Sure Admin, BT yöneticilerinin, ayarların hem uzaktan hem yerel yönetimi için parola yerine sertifikalar ve ortak anahtar şifreleme kullanarak hassas cihaz yazılım ayarlarını güvenle yönetmesini sağlar.

Yasal bilgiler

İkinci Basım: Ekim 2021

Birinci Basım: Aralık 2019

Belge Parça Numarası: L83995-142

İçindekiler

1 Başlarken

HP Sure Admin, BT yöneticilerinin, ayarların hem uzaktan hem yerel yönetimi için parola yerine sertifikalar ve ortak anahtar şifreleme kullanarak hassas cihaz yazılım ayarlarını güvenle yönetmesini sağlar.

HP Sure Admin aşağıdaki parçalardan oluşmaktadır:

- **Hedef Bilgisayar:** Geliştirilmiş BIOS Kimlik Doğrulama Modunu destekleyen yönetim platformları.
- **HP Manageability Integration Kit (MIK):** BIOS ayarlarının uzaktan yönetilmesi için System Center Configuration Manager (SCCM) veya HP BIOS Configuration Utility (BCU) eklentisi.
- **HP Sure Admin Local Access Authenticator:** Tek kullanımlık bir PIN almak için QR kodunu tarayarak BIOS kurulumuna yerel erişimi etkinleştirmek için parolayı değiştiren bir telefon uygulaması.

HP Sure Admin Kullanımı

Bu bölümde, HP Sure Admin kullanım süreci açıklanmaktadır.

1. System Configuration Manager (SCCM) veya Enhanced BIOS Configuration Utility (BCU) için HP Manageability Integration Kit (MIK) eklentisi içinde HP Sure Admin eklentisini açın.
2. HP Sure Admin telefon uygulamasını Google Play™ mağazasından veya Apple App Store®'dan indirin.
3. BIOS kilidini açmak üzere tek kullanımlık bir PIN almak için hedef cihaz ve HP Sure Admin telefon uygulaması tarafından kullanılan bir anahtar çifti oluşturun.

HP Sure Admin'i Devre Dışı Bırakma

Bu bölümde HP Sure Admin'i devre dışı bırakma seçenekleri açıklanmıştır.

- BIOS F10 ayarında **Güvenlik Ayarlarını Fabrika Varsayılan Ayarlarına Geri Yükle** öğesini seçin.

NOT: Bunun için F10 ayarlarına erişmek amacıyla HP Sure Admin telefon uygulaması üzerinden kimlik doğrulama PIN'i almak için kullanıcının fiziksel olarak orada bulunması gerekir.

- **Güvenlik Ayarlarını Fabrika Varsayılan Ayarlarına Geri Yükle** işleminin WMI'sını uzaktan çağırmak için BCU komutu kullanın.

NOT: Daha fazla bilgi için HP BIOS Configuration Utility (BCU) Kullanıcı Kılavuzuna bakın.

- MIK Güvenliği Sağlama sayfasında **Yetkilerin Kaldırılması** öğesini seçin.

2 Anahtar oluşturma ve yönetme

Geliştirilmiş BIOS Kimlik Doğrulama Modunu etkinleştirmeden önce MIK içinde Güvenliği Sağlama işlemini gerçekleştirin. Anahtar oluşturmak ve dışa aktarmak için Geliştirilmiş BIOS Kimlik Doğrulama Modu etkinleştirilmelidir. BIOS Kimlik Doğrulama Modunu etkinleştirmek için:

▲ Anahtar oluşturmak ve dışa aktarmak için HP Sure Admin eklentisini açıp **Geliştirilmiş BIOS Kimlik Doğrulama Modu** öğesini seçin.

Anahtar oluşturma ve dışa aktarma

Yerel erişim anahtarı çiftleri oluşturma ve tuşa erişim sağlamak için HP Sure Admin telefon uygulamasını etkinleştirmenin 3 farklı yolu vardır:

- Anahtar oluşturma ve manuel dağıtım ile aktarma, sayfa 2
- Azure AD İptali ile anahtar oluşturma ve dışa aktarma, sayfa 3
- Anahtar oluşturmak ve Azure AD Grubu OneDrive'a göndermek, sayfa 3

Anahtar oluşturma ve manuel dağıtım ile aktarma

Yerel erişim yetkilendirme anahtarını dışa aktarmak ve ardından e-posta üzerinden veya başka bir yöntemle HP Sure Admin telefon uygulamasına manuel olarak dağıtmak için bu seçeneği kullanın.

NOT: Bu seçenek, tek kullanımlık bir PIN almak için HP Sure Admin telefon uygulamasının ağa erişmesini gerektirmez.

1. Anahtarınızın adını **Anahtar Adı** kutusuna girin.
2. Parolayı **Parola** kutusuna girin.

   NOT: Parola, dışa aktarılan anahtarı korumak için kullanılır ve HP Sure Admin telefon uygulaması kullanıcısının anahtarı içe aktarabilmesi için sağlanması gerekir.

3. **Gözat** öğesini seçin ve sistemde yolun dışa aktarılacağı konumu seçin.
4. **Anahtar Oluştur** öğesini seçin. **Anahtar Oluştur** öğesinin yanında **Anahtar başarıyla oluşturuldu** mesajıyla birlikte bir bildirim simgesi belirdiğinde, anahtarınız başarıyla oluşturulmuştur.
5. **İleri**'yi seçin. Özet sayfasında, girdiğiniz HP Sure Admin ayarları görüntülenir.
6. **Politikayı Kaydet** öğesini seçin. **Başarıyla kaydedildi** mesajı göründüğünde politika kaydedilmiştir.
7. Anahtarı kaydettiğiniz klasöre gidin ve anahtarı, ilgili cihazda kullanıcının erişebileceği bir yöntemle (e-posta gibi) HP Sure Admin telefon uygulaması kullanıcısına dağıtın. Bu kullanıcı, anahtarı içe aktarmak için de parolaya ihtiyaç duyar. HP, anahtar ve parola için farklı dağıtım araçlarını kullanmanızı tavsiye eder.

   NOT: QR kodunu orijinal boyutunda gönderin. Uygulama, boyutu 800 × 600'den daha küçük olan görüntüleri doğru şekilde okuyamaz.

Azure AD İptali ile anahtar oluşturma ve dışa aktarma

Yerel erişim anahtarını belirtilen bir Azure Active Directory grubuna bağlamak ve HP Sure Admin telefon uygulamasının, yerel erişim PIN'i sağlamadan önce hem Azure Active Directory için kullanıcı kimlik doğrulaması yapılmasını hem de kullanıcının belirtilen grubun üyesi olduğunun onaylanmasını gerektirecek şekilde ayarlamak için bu seçeneği kullanın. Bu yöntem ayrıca, yerel erişim yetkilendirme anahtarının e-posta üzerinden veya başka bir yöntemle telefon uygulamasına manuel olarak dağıtılmasını gerektirir.

NOT: Bu seçenek, HP Sure Admin telefon uygulamasının tek kullanımlık bir PIN almak için ağ erişimine sahip olmasını gerektirir.

1. Anahtarınızın adını **Anahtar Adı** kutusuna girin.
2. Parolayı **Parola** kutusuna girin.

   NOT: Parola, dışa aktarılan anahtarı korumak için kullanılır ve HP Sure Admin telefon uygulaması kullanıcısının anahtarı içe aktarabilmesi için sağlanması gerekir.

3. **Azure AD Oturumu Açma** öğesini seçip oturum açın.
4. **Azure AD Grubu Adı** açılır kutusundan grubunuzun adını seçin. Anahtara erişim sağlamak için grubun üyesi olmanız gerekir.
5. **Gözat** öğesini seçin ve sistemde yolun dışa aktarılacağı konumu seçin.
6. **Anahtar Oluştur** öğesini seçin. **Anahtar Oluştur** öğesinin yanında **Anahtar başarıyla oluşturuldu** mesajıyla birlikte bir bildirim simgesi belirdiğinde, anahtarınız başarıyla oluşturulmuştur.
7. **İleri**'yi seçin. Özet sayfasında, girdiğiniz HP Sure Admin ayarları görüntülenir.
8. **Politikayı Kaydet** öğesini seçin. **Başarıyla kaydedildi** mesajı göründüğünde politika kaydedilmiştir.
9. Anahtarı kaydettiğiniz klasöre gidin ve anahtarı, ilgili cihazda kullanıcının erişebileceği bir yöntemle (e-posta gibi) HP Sure Admin telefon uygulaması kullanıcısına dağıtın. Bu kullanıcı, anahtarı içe aktarmak için de parolaya ihtiyaç duyar. HP, anahtar ve parola için farklı dağıtım araçlarını kullanmanızı tavsiye eder.

   NOT: QR kodunu orijinal boyutunda gönderin. Uygulama, boyutu 800 × 600'den daha küçük olan görüntüleri doğru şekilde okuyamaz.

Anahtar oluşturmak ve Azure AD Grubu OneDrive'a göndermek

(Tavsiye edilir) Yerel erişim yetkilendirme anahtarını telefonda depolamaktan kaçınmak için bu seçeneği kullanın. Bu seçeneği belirlediğinizde MIK, yerel erişim yetkilendirme anahtarını yalnızca yetkili grup tarafından erişilebilen, belirtilen OneDrive klasöründe depolayacaktır. PIN alınması gereken her durumda Azure AD kimliğini doğrulamak için HP Sure Admin telefon uygulaması gerekli olacaktır.

1. Anahtarınızın adını **Anahtar Adı** kutusuna girin.
2. Parolayı **Parola** kutusuna girin.
3. **Azure AD Oturumu Açma** öğesini seçip oturum açın.
4. Azure AD Grubu Adı açılır kutusundan grubunuzun adını seçin.

   NOT: Anahtara erişim sağlamak için grubun üyesi olmanız gerekir.

5. Anahtarın kaydedilmesini istediğiniz OneDrive klasörünün adını **OneDrive** kutusuna girin.

6. **Gözat** öğesini seçin ve sistemde yolun dışa aktarılacağı konumu seçin.

7. **Anahtar Oluştur** öğesini seçin.

NOT: **Anahtar Oluştur** öğesinin yanında, **Anahtar başarıyla oluşturuldu** mesajıyla birlikte bir bildirim simgesi belirdiğinde anahtarınız, belirtilen OneDrive klasörüne başarıyla eklenir ve belirtilen yerel klasöre aktarılır.

8. **İleri**'yi seçin. Özet sayfasında, girdiğiniz HP Sure Admin ayarları görüntülenir.

9. **Politikayı Kaydet** öğesini seçin. **Başarıyla kaydedildi** mesajı göründüğünde politika kaydedilmiştir.

NOT: Bu senaryoda, ön onay almak için HP Sure Admin telefon uygulamasına hiçbir şey göndermeniz gerekmez. Hedef bilgisayarlar, QR kodunda bulunan OneDrive konumu bilgisine işaret etmek üzere sağlanır. HP Sure Admin telefon uygulaması, kullanıcı yetkili grubun bir parçasıysa ve kimliği başarıyla onaylanırsa OneDrive konumuna erişmek için bu işaretçiyi kullanır.

3 Telefon kurulumu

HP Sure Admin telefon uygulamasını Google Play veya Apple Store'dan indirin.

- Android telefonlar için Google mağazasından HP Sure Admin'i indirin.
- iOS telefonlar için Apple Store'dan HP Sure Admin'i indirin.

HP Sure Admin telefon uygulamasını kullanarak BIOS kilidini açma

HP Sure Admin mobil uygulaması, hedef makine tarafından sunulan QR kodunu tarama yoluyla elde edilen tek kullanımlık bir PIN sağlayarak BIOS kurulumuna yerel erişim için kullanılan BIOS parolasının yerini alır.

Anahtarın telefon uygulaması kullanıcısına gönderildiği bir senaryodaki anahtarı yerel olarak telefona kaydetmek için bu adımları uygulayın. Aşağıdaki örnekte anahtar, HP Sure Yönetici telefon uygulaması kullanıcıya e-posta ile gönderilmiştir ve kullanıcı telefonda e-postayı açar.

1. Anahtarı içeren e-postayı açın.
2. **Kayıt** sayfası görüntülenirken, anahtarın şifresini çözmek ve HP Sure Admin uygulamasına eklemek için **Parolayı girin** kutusuna ve e-posta adresinizi **E-posta adresinizi girin** kutusuna girin. Kilit açma PIN'i numaranız, **PIN'iniz** sayfasında görüntülenir.

   NOT: Bu adım, anahtarı mobil cihaza kaydeder ve kaydı tamamlar. Bu noktada, bu anahtarla erişilebilecek şekilde hazırlanmış olan tüm cihazlara erişim sağlamak için HP Sure Admin telefon uygulamasını kullanabilirsiniz. E-posta adresi yalnızca yöneticinin talep etmesi halinde gereklidir.

3. PIN'i **BIOS Yanıt Kodunu Girin** kutusuna girin.

Kayıt sonrasında BIOS kurulumuna erişim sağlama

Kayıttan sonra bir hedef makinede BIOS kurulumuna erişim sağlamak için:

1. Hedef makinede önyükleme sırasında BIOS kurulumuna girin.
2. Telefon uygulamasındaki **QR Kodu Tara** öğesini seçin ve hedef makinedeki QR kodunu tarayın.
3. Kullanıcının kimliğini doğrulamak için istenirse kimlik bilgilerinizi sunun.
4. Kilitli olmayan PIN numarası, **PIN'iniz** sayfasında görüntülenir.
5. PIN'i, hedef makinedeki **BIOS Yanıt Kodunu Girin** kutusuna girin.

Azure AD Grubu OneDrive ile BIOS'un kilidini açma

Azure AD Grubu OneDrive ile BIOS kilidini açmak üzere HP Sure Admin'i kullanmak için:

1. **QR Kodu Tara** öğesini seçin ve ardından BIOS QR kodunu tarayın.

   NOT: HP Sure Admin uygulamasında Azure AD oturum açma sayfası görüntülenir.

2. Azure hesabınızda oturum açın.

3. PIN'i **BIOS Yanıt Kodunu Girin** kutusuna girin.

NOT: Bu senaryoda HP Sure Admin uygulaması, anahtarı yerel olarak kaydetmez. Tek kullanımlık PIN alınması gereken her durumda HP Sure Admin telefon uygulamasının ağ erişimine sahip olması ve kullanıcının kimliğini doğrulaması gerekir.

4 HP Sure Admin hata kodları

HP Sure Admin ve KMS Admin Console hata kodlarını, türlerini ve açıklamalarını görmek için bu bölümdeki tabloyu kullanın.

Tablo 4-1 HP Sure Admin uygulaması hata kodları, türleri ve bunların açıklamaları

Hata kodu	Hata Türü	Açıklama
100	QRCodeUnknownError	Genel hata.
101	QRCodeDeserialization	QR Kodu JSON okunamıyor. Dize geçerli bir JSON dosyası değil veya veri geçersiz.
102	QRCodeInvalidImage	Taranan QR Kodu görüntüsü geçersiz. QR Kodu görüntü dosyası okunamıyor.
103	QRCodeNoPayload	Taranan QR Kodu görüntüsü geçersiz. Görüntü dosyasında JSON yükü yok.
104	QRCodeInvalid	QR Kodu JSON okunamıyor. Dize geçerli bir JSON değil veya QR görüntüsündeki veri geçersiz.
105	QRCodeInvalidKeyIdHash	QR Kodu JSON'daki genel anahtar karma kodu, kayıt paketindeki genel anahtar karma kodu (KeyID verisi) ile eşleşmiyor.
106	QRCodeTampered	Taranan QR Kodu görüntüsü bozulmuş veya geçersiz.
107	QRCodeTamperedOrInvalidPassPhrase	Taranan QR Kodu görüntüsü bozulmuş ve geçersiz ya da girilen şifre yanlış.

Tablo 4-2 OneDrive hataları, türleri ve açıklamalarından OneTime erişim tuşu

Hata kodu	Hata türü	Açıklama
200	OneTimeKeyError	Genel hata.
201	OneTimeKeyNoUserGroups	Oturum açan kullanıcı, kuruluşunuzdaki herhangi bir AD grubuna ait değil.
203	OneTimeKeyInvalidUserGroup	Oturum açan kullanıcı, bu anahtarın atandığı AD Grubuna ait değil.
204	OneTimeKeyQRFileDoesNotExist	Tek kullanımlık anahtar dosyası, AD Grubunun OneDrive klasöründe yok.
205	OneTimeKeyInvalidQRFile	AD Grubunun OneDrive klasöründeki tek kullanımlık anahtar dosyası geçersiz.
206	OneTimeKeyInvalidQRpayload	Tek kullanımlık anahtar dosyası var ancak dosya yükü okunamıyor.

Tablo 4-3 Azure AD Yetkilendirme hataları

Hata kodu	Hata türü	Açıklama
300	AzureADUnknownError	Genel hata.
301	AzureADInvalidDomain	Girilen e-posta adresi, QR Kodu görüntüsünde belirtilen etki alanı adı ile eşleşmiyor.
302	AzureADAccessToken	Azure AD'den erişim belirteci alınırken hata oluştu. Kullanıcı, kuruluşunuzun Azure AD hizmetinde oturum açamıyor veya uygulama, kuruluşunuzun Azure AD hizmetiyle bağlanması için gerekli izinlere sahip değil. Kullanıcı kimlik doğrulamayı iptal etmiş de olabilir.
303	AzureADUserProfile	HP Sure Admin uygulaması, kuruluşunuzun Azure AD hizmetinden Kullanıcı profili bilgisi almak üzere yetkilendirilmişti.
304	AzureADUserPrincipalMismatch	Girilen e-posta adresi, oturum açan kullanıcının asıl adıyla eşleşmiyor.
305	AzureADUserInvalidUserGroup	Oturum açan kullanıcı, bu anahtarın atandığı atanan Azure AD Grubuna ait değil.

Tablo 4-4 KMS Admin Console hataları, türleri ve açıklamaları

Hata kodu	Hata türü	Açıklama
401	KmsUnauthorized	Kullanıcının KMS hizmetini kullanma yetkisi yok.
402	KmsKeyDoesNotExist	Eşleşen özel anahtar KMS anahtar kasasında yok. Tuş şu anda silinmiş ancak kurtarılabilir durumda ve adı bu durumda yeniden kullanılamaz. Anahtar yalnızca kurtarılabilir veya temizlenebilir.
403	KmsKeyDoesNotExistInTableStorage	Anahtar tablo deposunda yok.
404	KmsUploadKeyErrorInKeyVault	Anahtar kasasına anahtar eklenirken hata oluştu.
405	KmsUploadKeyUnauthorized	Kullanıcı anahtarları yükleme yetkisine sahip değil. Kullanıcı, bu API'yi aramasına izin verilen yetkili AD Grubuna ait değil.
406	KmsInvalidAzureADLogin	Kullanıcı Azure Tenant AAD'de oturum açmamış.
407	KmsNoUserGroups	Oturum açan kullanıcı, kuruluşunuzdaki herhangi bir AD Grubuna ait değil.
408	KmsInvalidUserGroup	Oturum açan kullanıcı, bu anahtarın atandığı AD Grubuna ait değil.
409	KmsInvalidAccessToken	İstekte sağlanan erişim belirteci geçersiz.
410	KmsAccessTokenExpired	Sağlanan erişim belirtecinin süresi dolmuş.
411	KmsAccessTokenInvalidTenantId	Sağlanan erişim belirtecinde Geçersiz Kiracı Kimliği değeri var.

Tablo 4-4 KMS Admin Console hataları, türleri ve açıklamaları (devam)

Hata kodu	Hata türü	Açıklama
412	KmsAccessTokenTenantIdMismatch	Sağlanan erişim belirtecindeki Kiracı Kimliği, işlev uygulaması Kiracı Kimliğiyle eşleşmiyor.
413	KmsInvalidKeyId	Anahtar kimliği değersiz veya boş.
414	KmsDeleteKeyUnauthorized	Kullanıcı anahtarları silme yetkisine sahip değil. Kullanıcı, bu API'yi aramasına izin verilen yetkili AD Grubuna ait değil.
415	KmsKeyVaultSoftDeleteUnrecoverableState	Gizli sürücüyü kurtarma girişimi başarısız oldu ve kurtarılamadı. Kullanıcı yeniden denemelidir.
416	KmsInvalidGetKeysRequest	Anahtar alma isteği geçersiz.
417	KmsGetKeysAyarısız	Kullanıcı anahtar alma yetkisine sahip değil. Kullanıcı, bu API'yi aramasına izin verilen yetkili AD Grubuna ait değil.
418	KmsInvalidRequestPayload	API tarafından alınan istek geçersiz.
419	KmsRequestRequired	Alınan istek boş olmamalıdır.
420	KmsKeyNotConcurrent	Tablo deposundaki anahtar, kullanıcı son kez bir kopya aldıktan sonra güncelleştirildi veya değiştirildi.